SESAR Solution PJ.01-06 SPR-INTEROP/OSED V3 - Part II - Safety Assessment Report

Deliverable ID:	D5.1.010
Dissemination Level:	PU
Project Acronym:	PJ.01 EAD
Grant:	731864
Call:	H2020-SESAR-2015-2
Topic:	ENHANCED ARRIVALS AND DEPARTURES
Consortium Coordinator:	NATS
Edition Date:	22 November 2019
Edition:	00.04.00
Template Edition:	02.00.01

Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
Tobias Finck / DLR	Document Lead	22 November 2019

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
Thomas Lueken / DLR	Solution Lead	15 June 2019
Thomas Lueken / DLR	Solution Lead	18 July 2019
Thomas Lueken / DLR	Solution Lead	22 November 2019
Sven Schmerwitz / DLR	Project Member	22 November 2019
Omkar Halbe / AHD	Project Member	22 November 2019
Roland Bonel / Thales	Project Member	22 November 2019

Approved for submission to the SJU By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
Thomas Lueken / DLR	Solution Lead	22 November 2019

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date

Document History

Edition	Date	Status	Author	Justification
00.00.01	06 June 2019	Version for review	Tobias Finck	
00.01.00	18 July 2019	Final Version	Tobias Finck	
00.02.00	03 Sept 2019	Preparation for resubmission	Thomas Lueken Tobias Finck	
00.03.01	19Nov 2019	Reopened document after V3 Gate Meeting	Tobias Finck	
00.04.00	22 Nov 2019	Resubmitted document	Tobias Finck	Comments from Bruno Rabiller included

Copyright Statement

PJ.01 EAD

ENHANCED ARRIVALS AND DEPARTURES

This SPR-INTEROP/OSED (Part II) deliverable is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 731864 under European Union's Horizon 2020 research and innovation programme.

Abstract

This document is the final V3 Safety Assessment Report for Solution PJ.01-06 during Wave 1 of SESAR2020. The work performed was to assess and validate the benefit of integrating piloting supporting enhanced vision systems that can increase the safety and reliability of rotorcraft operations through dedicated symbology for specific rotorcraft operations, especially during arrival and departure operations including visual segments. The objective was to assess and validated the benefit of having SBAS based navigation for advanced Point-In-Space RNP approaches and departures to/from FATO by defining the corresponding rotorcraft specific contingency procedures in case of loss of communication. As the SBAS navigation, the corresponding contingency procedures will need to comply as much as possible with profiles adapted to exploit rotorcraft performances, reduce fuel consumption and noise emission. The pilot was supported during these operations by dedicated symbology presented on a Head Mounted Display system.

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ.01-06 Solution in TMA operations. The report presents the assurance that the Safety Requirements for the V1-V3 phases are complete, correct and realistic, thereby providing all material to adequately inform the V3 PJ.01-06 Solution SPR-INTEROP/OSED.

Based on the Safety Criteria which were already defined in the PJ.01-06 V3 VALP Part II (Safety Assessment Plan) this document contains the appropriate Safety Objectives and Requirements. Safety Objectives have been defined for normal and abnormal conditions as well as for the failure approach.

Taking into account the use cases defined in SPR-INTEROP/OSED Part I and a new SPR-level model defined during this Safety Assessment, Safety Requirements have been defined for each Safety Objective. In the case of internal system failures, a cause analysis was performed with the definition of fault trees.

2 Introduction

2.1 Background

SESAR Solution PJ.01-06 is part of PJ.01. The aim of the solution was to assess and validate the benefit of integrating piloting supporting enhanced vision systems that can increase the safety and reliability of rotorcraft operations through dedicated symbology for specific rotorcraft operations including visual segments. The objective was to assess and validate the benefit of having SBAS based navigation for advanced Point-In-Space RNP approaches and departures to/from FATO by defining the corresponding rotorcraft specific contingency procedures in case of loss of communication. As the SBAS navigation, the corresponding contingency procedures have been complied as much as possible with profiles adapted to exploit rotorcraft performances, reduce fuel consumption and noise emission. The pilot has been supported during these operations by dedicated symbology presented on a Head Mounted Display system.

2.2 General Approach to Safety Assessment

The general approach of the Safety Assessment based on the SESAR "Safety – Guidance Reference Material" is described in Table 1.

V-level	Description
V1 level	• Analysis of the operational environment and development of the safety criteria on the basis of the relevant En-Route and Controlled Flight into Terrain (CFIT) Accident Incident Models (AIM)
V2 level phase one	• Focus on the solution concept • Derivation of the Safety Objectives (success and failure) in support of the Safety Criteria • Describing of the Safety Objectives at OSED level
V2 level phase two	• Analysis of the SPR level model • Derivation of the Safety Requirements (success and failure) in support of the Safety Objectives (success and failure) • Documentation of the Safety Requirements (success and failure) and the allocation process in the V2 SPR document
V3 level	• Analysis of a physical model to represent the planned final design solution • Derivation of low level physical Safety Requirements • Documentation of safety related human performance tasks in the V3 SPR • Documentation of the safety related technical elements in the TS document

Table 1: SESAR2020 - Safety lifecycle

2.3 Scope of the Safety Assessment

Solution PJ.01-06 started at V3 level so the given lifecycle has been slightly adapted to meet all necessary parts of the Safety Assessment.

This Safety Assessment Report describes the V3 Safety Results of the Solution. Safety Objectives and Safety Requirements are part of the V3 Safety Assessment and are described in this Safety Assessment Report of the SPR-INTEROP/OSED.

For each Safety Objective identified in Chapter 3, Chapter 4 defines Safety Requirements that must ensure that the concept of advanced PinS operations is as safe as the current operational procedures.

Table 2 lists the general safety roles and responsibilities for solution PJ.01-06.

Actors	Tasks
PJ.01 Safety Focal Point	Guarantee of homogeneous safety standards in the different solutions of PJ.01.
PJ.01-06 Solution Lead	Planning and coordination of safety activities within the solution and monitoring of the documentation (VALP/VALR).
PJ.01-06 Validation Report (VALR) Lead	Consideration of the identified safety aspects in the conducted validation exercises.
PJ.01-06 SPR-INTEROP/OSED Lead	Consideration of the identified safety aspects in the Operational Environment as well as the Safety and Performance Requirements.
PJ.01-06 Human Performance Assessment Lead	Planning and coordination of human performance related safety activities within the solution and monitoring of the documentation
PJ.01-06 Exercise Leads	Identification of safety-relevant changes in their validation exercises.

Table 2: Safety roles and responsibilities for PJ.01-06 Safety Activities

The intended audience for this document are the team members of PJ.01-06, including other PJ.01 Solutions:

- PJ.01-01 – Extended Arrival Management with overlapping AMAN operations and interaction with DCB
- PJ.01-02 – Use of Arrival and Departure Management Information for Traffic Optimisation within the TMA
- PJ.01-03a – Improved Parallel Operations
- PJ.01-03b – Dynamic E-TMA for Advanced Continuous Climb and Descent Operations
- PJ.01-05 – Airborne Spacing Flight Deck Interval Management
- PJ.01-07 – Approach Improvement through Assisted Visual Separation

Also those from the following SESAR Solutions:

- PJ.02-05 Independent Rotorcraft IFR operations at the Airport
- PJ.06-02 Management of Performance Based Free Routing in lower Airspace

From the Technical SESAR 2020 Solutions:

- PJ.18-02a A/G exchanges for RBT management

And following transverse and federating projects:

- PJ.19

2.4 Layout of the Document

Section 1 provides an Executive Summary of the Safety Assessment Report (SAR).

Section 2 gives an overview of the Safety Assessment Concept in general and in Solution PJ.10-01b.

Section 3 gives an overview of the safety specifications at the OSED level.

Section 4 gives an overview of the safe design at SPR level.

Section 5 describes the used acronyms and terminology of this document.

Section 6 lists all the documents referred to in this SPR-INTEROP/OSED Part II - Safety Assessment Report.

Appendix A lists the defined Safety Objectives of the Solution.

Appendix B lists the consolidated Safety Requirements of the Solution.

Appendix C lists the identified assumptions, safety issues and operational limitations of the Solution.

Appendix D lists the Safety Assurance Activities (SAA) to inform the OSED section of the SPR-INTEROP/OSED as well as the Safety Assurance Activities to inform the SPR section of the SPR-INTEROP/OSED.

3 Safety specifications at the OSED Level

3.1 Scope

Chapter 3 addresses the following activities:

- Description of the key properties of the Operational Environment that are relevant to the safety assessment – section 3.2
- Identification of the pre-existing hazards that affect traffic in the Solution relevant operational environment (airspace, airport) and the risks of which operational services provided by the Solution may reasonably be expected to mitigate to some degree and extent – section 3.3
- Identification of all relevant pre-existing hazards – section 3.4
- Setting of the Safety Criteria (from the Solution Safety Plan, Reference) – sections 3.5
- Comprehensive determination of the operational services that are provided by the Solution to address the relevant pre-existing hazards and derivation of Safety Objectives (success approach) in order to mitigate the pre-existing risks under normal operational conditions – section 3.6
- Assessment of the adequacy of the operational services provided by the Solution under abnormal conditions of the Operational Environment – section 3.7
- Assessment of the adequacy of the operational services provided by the Solution in the case of internal failures and mitigation of the System-generated hazards (derivation of Safety Objectives (failure approach)) – section 3.8
- Analysis of the impact of Solution PJ.10-01b operations on adjacent airspace or on neighbouring sectors – section 3.9
- Achievability of the Safety Criteria – section 3.10
- Validation & verification of the safety specification – section 3.11

3.2 PJ.01-06 Solution Operational Environment and Key Properties

Table 3 shows the differences between the current and new operating methods regarding vertical guidance and curves in PinS.

Activities (in EATMA) that are impacted by the SESAR Solution	Current Operating Method	New Operating Method
Acknowledge landing clearance	The rotorcraft pilot receives the landing clearance and confirms this with a read back	

Arrival traffic control and sequencing	The executive approach and departure controller is responsible for the arrival traffic including sequencing.	
Change frequency and contact Executive Approach/Departure Controller	After receiving handover information the pilot contacts the executive approach and departure controller	
Change to TWR frequency	After receiving handover information the rotorcraft pilot switches his frequency to the TWR controller	
Clear flight for cruise	The executive approach and departure controller clears the rotorcraft for cruise flight level.	
Control departure traffic	The TWR controller controls the departure traffic under his responsibility	
Cruise flight without HMD, with head-down display	N/A	After reaching cruise flight level, the pilot flies without HMD and with head-down display
Flight according PinS take-off trajectory with HMI	N/A	After IFR clearance the rotorcraft flies PinS take-off trajectory with HMD until he reaches cruise flight level.
Flight with head-down display	N/A	The pilot flies with head-down display until he reaches IAF
Monitor trajectory until MAPt	The pilot monitors the trajectory until he reaches MAPt	
Preform missed approach procedure	If no visual reference is available at MAPt or the pilot decides not to land, the rotorcraft performs a missed approach procedure	
PinS approach with HMD	N/A	After reaching IAF the pilot flies a PinS approach with HMD
Provide departure clearance (advanced PinS procedure)	N/A	The TWR controller provides departure clearance with advanced PinS
Provide landing clearance (advanced PinS procedure)	N/A	The TWR controller provides a landing clearance to the rotorcraft crew
Request departure clearance (advanced PinS approach)	N/A	The Flight Crew requests departure clearance with advanced PinS
Rotorcraft complies to approach clearance	The rotorcraft complies to the given approach clearance	

Sequencing, Separation, Speed regulation	The executive approach and departure controller is responsible for sequencing, separation and speed regulation as long as the rotorcraft is under his responsibility	
Surveillance until MAPt	If the rotorcraft flies a missed approach procedure the TWR controller provides the handover information to the crew	
Transfer flight to TWR	After reaching FAF the controller provides handover information to the rotorcraft crew	
Transfer flight to Executive Approach/Departure Controller	After the rotorcraft reaches IDF the TWR controller provides handover information to the rotorcraft crew	
Visual departure with HMD until IDF	N/A	The pilot flies visual departure with HMD until he reaches IDF

Table 3: Difference between new and previous Operating Method

For further information about the details of change please refer to SPR-INTEROP/OSED Part I, Section 3.3.3.

3.3 Airspace Users Requirements

There is no change to the responsibilities of the Flight Crew regarding the safe conduct of the flight during PinS procedures. Flight crews are still responsible for the safe and efficient control and navigation of their individual aircraft in all airspaces. However, procedures will now include flight crews' use of the advanced on board avionics technologies, improving the decision-making process for the safe and efficient management of the flight. Taking this into account Safety shall still remain on the same level as for today's procedures.

3.4 Relevant Pre-existing Hazards

Table 4 shows the five possible pre-existing hazards for TMA identified in the Guidance to Apply the SESAR Safety Reference Material.

Pre-existing hazard	Description
Hp#1	a situation in which the intended trajectories of two or more rotorcraft/aircraft are in conflict
Hp#2	a situation where the intended trajectory of a rotorcraft is in conflict with terrain or an obstacle
Hp#3	penetration of restricted airspace
Hp#4	wake vortex encounters (WVE)
Hp#5	encounters with adverse weather

Table 4: Possible pre-existing hazards

With the new concept of SBAS based navigation for advanced Point-In-Space RNP approaches and departures to/from FATO with pilot HMD only Hp#2 “a situation where the intended trajectory of a rotorcraft is in conflict with terrain or an obstacle” is relevant.

3.5 Safety Criteria

Based on the Accident Incident Model Charts (AIM-Charts) for Controlled Flight into Terrain (CFIT) four Safety Criteria were defined to ensure that the new procedure increase Safety. Table 5 shows the defined Safety Criteria and the corresponding Barriers

Safety Criteria	Description
SAC101	The number of Controlled Flight Towards Terrain (CF4) shall remain the same with the new concept.
SAC102	The number of Flight Towards Terrain Commanded by Pilot (CF5) shall be reduced by the new concept due to the use of an HMD.
SAC103	The number of Flight Towards Terrain Commanded by System (CF6) shall remain the same with the new concept.

Table 5: Safety Criteria

No Safety Criteria associated to MAC were defined, as no differences compared to standard PinS operations for controlled airspace were identified by the solution.

3.6 Mitigation of the Pre-existing Risks – Normal Operations

3.6.1 Operational Services to Address the Pre-existing Hazards

This section describes the Solution Operational Services that are provided to address the pre-existing hazard (Hp#2 “a situation where the intended trajectory of a rotorcraft is in conflict with terrain or an obstacle”) identified above. For the following Operational Services changes due to the new operational concept are expected:

- Provide separation from terrain/obstacles

Table 6shows the link between the Operational Services described above and the identified relevant pre-existing hazards.

ID	Service Objective	Pre-existing Hazards [Hp#xx]
OS-001	Provide separation from terrain/obstacles	Hp#2

Table 6: ATM and Pre-existing Hazards

3.6.2 Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations

In this chapter the Safety Objectives for normal operations are defined. Normal conditions are defined as conditions which the system is expected to encounter in everyday operations with the following characteristics:

- Normal traffic flow
- Normal and stable weather conditions
- Different traffic situations regarding congested/decongested areas

Normal operation can be different from the geographical area in which it is to be applied. While in northern Europe, during the winter months, cold and snowfall is a normal weather situation, the average temperature in southern Europe in winter is much higher and snowfall is very seldom. Due to the fact that the exercises of Solution PJ.01-06 covers geographical regions of middle Europe this Safety Assessment covers normal operation as they are typical for this region.

Ref	Phase of Flight / Operational Service	Related AIM Barrier	Achieved by / Safety Objective [SO xx]
1	Provide separation from terrain/obstacles	B4 (CF4)	SO-0001
2	Provide separation from terrain/obstacles	B5 (CF5)	SO-0002
3	Provide separation from terrain/obstacles	B6 (CF6)	SO-0003

Table 7: PJ.01-06 Solution Operational Services & Safety Objectives (success approach)

Table 8 lists the defined Safety Objectives (success approach) for Normal Operations in order to achieve the identified Operational Services.

ID	Description
SO-0001	FCRW monitoring during advanced PinS operation shall be effective
SO-0002	Trajectory management by FCRW shall be effective during advanced PinS operation
SO-0003	Trajectory management by A/C systems shall be effective during advanced PinS operation

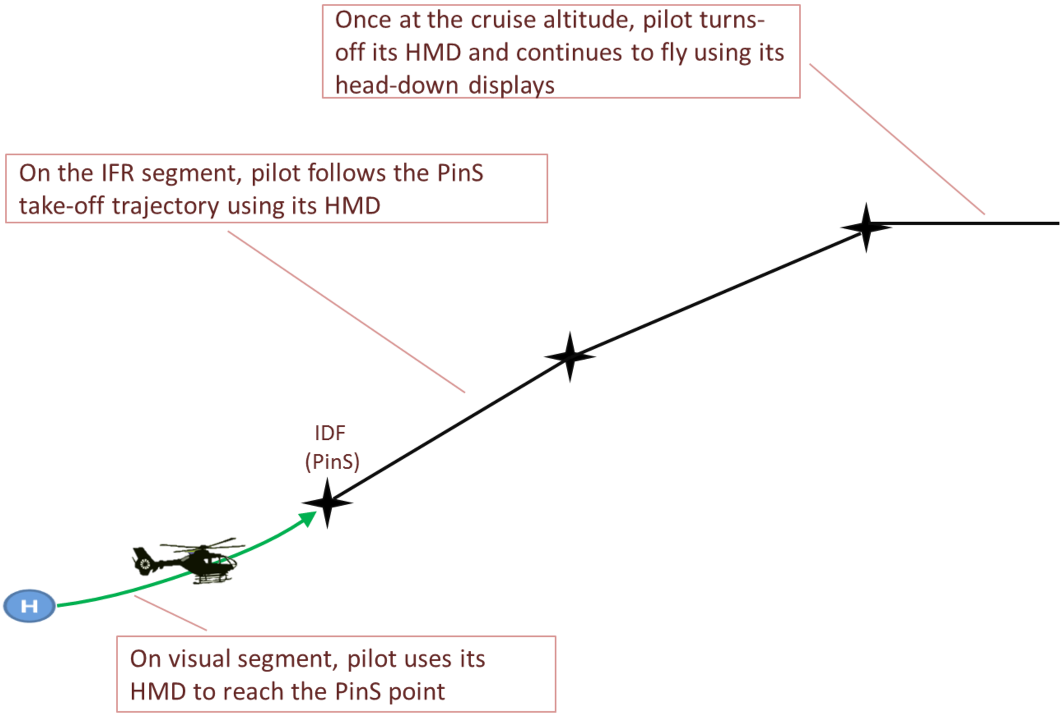
Table 8: List of Safety Objectives (success approach) for Normal Operations

3.6.3 Analysis of the Concept for a Typical Flight

In this chapter the completeness of the above derived safety objectives will be analysed by considering a typical normal flight as a continuous process and addressing in particular the transition modes. Additional safety objectives (functionality and performance) are described in Table 12.

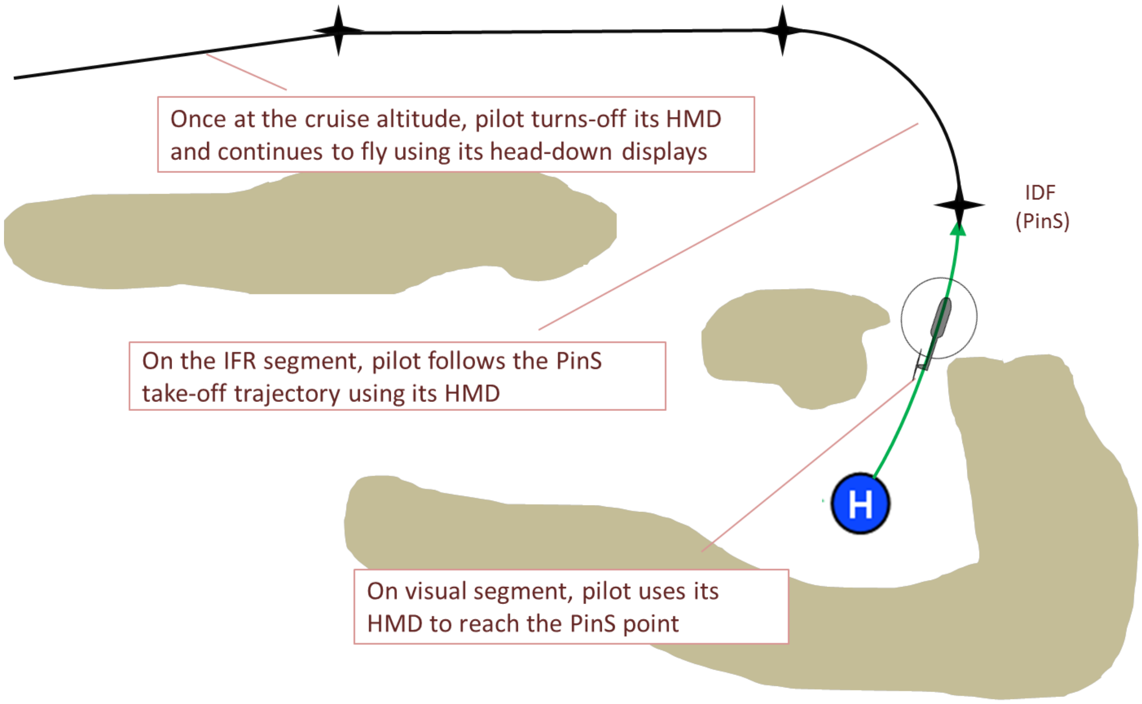
<u>**Departure Procedure:**</u>

Flying a PinS departure procedure consists first – for the pilot – to fly visually to the first point of the instrument procedure, the IDF (Initial Departure Fix), which is a navigation waypoint defined by geographic coordinates and a Minimum Crossing Altitude (MCA). As during this phase the pilot is flying "eyes-out", meaning looking outside to control separation with other traffic and with terrain and obstacles, the HMD can help him to navigate towards the IDF while keeping an eye on its piloting parameters (altitude, heading, speeds…).



PinS departure using HMD – Vertical profile

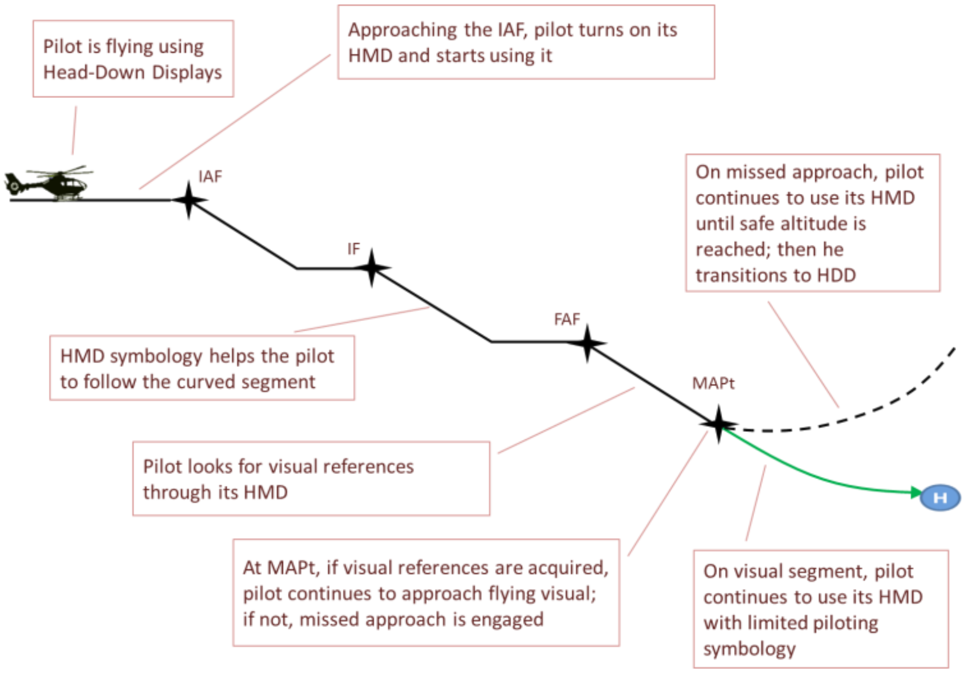
Once on the IFR segment, the pilot can continue to use its HMD to take benefit from the HMD symbology, in particular when this procedure is flown manually. Indeed, this manoeuver combines longitudinal, lateral and vertical movements, in particular on the curved part of the departure procedure. Once the cruise altitude has been reached, the pilot can turn-off its HMD and continue a normal instrument flight using its head-down displays.



PinS departure using HMD – Lateral profile

Arrival Procedure:

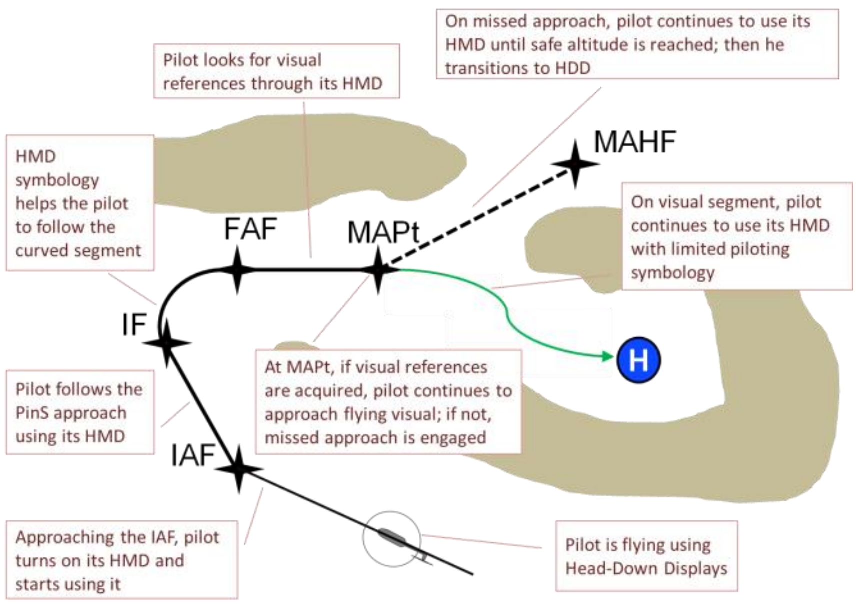
The helicopter is flying IFR on a route that can be any kind of RNP/RNAV route, including low-level RNP0.3 route specific to helicopter operations. At some distance from the first point of the PinS instrument approach, the IAF (Initial Approach Fix), the pilot turns ON his HMD. Once on the descent phase, the HMD symbology helps the pilot to control laterally and vertically the trajectory, as well as the flight parameters (speed, altitude, velocity vector…); a first recognition of the external scene is then possible (if weather conditions allow it); during the curved segment (between the IF – Intermediate Fix – and the FAF – the Final Approach Fix), which combines longitudinal, lateral and vertical movements, the HMD brings to the pilot means to control its trajectory while keeping an eye on the external scene.



PinS approach using HMD – Vertical profile

When approaching the MAPt (Missed Approach Point), at which a decision shall be taken by the pilot to continue or abort the approach, this is where the HMD is particularly helpful, allowing the pilot to acquire the necessary visual references defined by the approach chart while controlling the flight parameters and keeping the helicopter on the final approach segment.

During the final approach segment (ie. from FAF to MAPt), if the PinS approach is an LPV (Localizer Performance with Vertical guidance) approach, the HMD shall be used to display the lateral and vertical deviations compared to the Final Approach Segment (FAS).



PinS approach using HMD – Lateral profile

At the MAPt:

- If the visual references have been acquired visually (through the HMD), then the pilot continues to fly towards the landing zone (LZ), either under VFR regime (in case of a "Proceed VFR" procedure) or "visually" under IFR regime (in case of a "Proceed Visually" procedure. During this visual segment, the pilot continues (if he considers this display as helpful) to use the HMD to navigate towards the LZ, controlling in particular its airspeed, heading and height above ground).
- If the minimum visual references have not been acquired visually, then the pilot initiates a "go-around", and continues to use the HMD to fly the missed-approach procedure. When the safety altitude has been reached, the pilot can choose to fly to an alternate destination or to perform a second round of the approach. In the first case, depending on the distance to the alternate destination, the pilot may decide to turn OFF its HMD and fly "head-down", or continue to fly "eyes-out" with its HMD; in the last case, he will probably prefer to continue to use the HMD since the return to the approach path is relatively short.

No additional Safety Objectives (success approach) for a typical flight (departure procedure and arrival procedure) were identified.

3.7 PJ.01-06 Solution Operations under Abnormal Conditions

The purpose of this section is to assess the ability of the Solution to work through (robustness), or at least recover from (resilience) any abnormal conditions, external to the Solution System, that might be encountered relatively infrequently.

3.7.1 Identification of Abnormal Conditions

The following abnormal conditions are relevant in the new concept:

- Loss of GNSS/SBAS (interference, Ionospheric disturbances)
- Severe weather conditions (e.g. thunderstorm, strong wind)

3.7.2 Potential Mitigations of Abnormal Conditions

In this chapter the abnormal conditions identified above, will be further analysed. Table 9 shows for each abnormal condition, the assessed immediate operational effect and the possible mitigations of the safety consequence of the operational effect with a reference to existing safety objectives (as per Table 8 and **Error! Reference source not found.**) or to new safety objectives described in Table 10 below.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
1	Loss of GNSS/SBAS	(Interference or Ionospheric disturbances can led to a loss of GNSS/SBAS	SO-0004

2	Severe weather conditions (DVE)	Severe weather conditions can led to a missed approach procedure	SO-0005

Table 9: Additional Safety Objectives (success approach) for Abnormal Conditions

The following additional Safety Objectives (success approach) were defined to cover the abnormal conditions identified above.

ID	Description
SO-0004	FCRW shall revert to contingency procedures in case of loss of GNSS during advanced PinS operation
SO-0005	FCRW shall be supported by HMD in case of DVE

Table 10: List of Safety Objectives (success approach) for Abnormal Operations

3.8 Mitigation of System-generated Risks (failure approach)

This section concerns Solution operations in the case of internal failures. Before any conclusion can be reached concerning the adequacy of the safety specification of Solution operations, at the OSED level, it is necessary to assess the possible adverse effects that failures internal to the end-to-end Solution System might have upon the provision of the relevant operational services described in section 3.6.1 and to derive safety objectives (failure approach) to mitigate against these effects.

3.8.1 Identification and Analysis of System-generated Hazards

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Severity *(most probable effect)*
Hz-001	Helicopter deviates from advanced PinS towards terrain/obstacle	SO-0001 SO-0002 SO-0003 SO-0004 SO-0005	Helicopter might collide with terrain/obstacle following lateral or vertical deviation	ATCO detection MSAW Pilot visual avoidance HTAWS	SC3a

Table 11: System-Generated Hazards and Analysis

Table 12 shows additional Safety Objectives (functionality and performance) which shall mitigate the defined hazards in case of internal failures. Each hazard scenario and the corresponding Safety Requirements are described more in detail in Chapter 4.6.

ID	Description
SO-0006	FCRW shall revert to contingency procedures in case of loss of HMD during advanced PinS operation.
SO-0007	FCRW shall revert to contingency procedures in case of loss of AP during advanced PinS operation

Table 12: Additional Safety Objectives (functionality and performance) in the case of internal failures

3.8.2 Derivation of Safety Objectives (integrity/reliability)

The following Safety Objectives (integrity and reliability) defined in Table 15 describe the frequency limitation with which the above Solution System generated hazards could be allowed to occur. For the determination and mathematical calculation the relevant Risk Classification Scheme(s) from Guidance E.3 and SO mathematical calculation guidance in Guidance E.4 of Guidance to Apply the Safety Reference Material were used.

The calculation is done via the following formula:

$$SO = \frac{MTFoO_{relevant\_severity\_class}}{N\ x\ IM}$$

$MTFoO_{relevant\_severity\_class}$: Maximum Tolerable Frequency of Occurrence being the maximum probability of the hazard's effect

N: Overall number of operational hazards for a given severity class at a given barrier

IM: Impact Modification factor to take account of additional information regarding the operational effect of the hazard

In general the Impact Modification factor has a reference value of IM = 1. In case of a very high impact of a barrier failure and in case a hazard involves multiple (many aircraft) a higher value i.e. IM = 10 can be used.

Table 13 shows the number of hazards per Severity Class for Mid-air collision in En-Route as well as Controlled Flight into Terrain.

Severity Class	Number of hazards per Severity Class per Accident Type (CFIT)
SC1	5
SC2	10
SC2a	N/A
SC2b	N/A
SC3	N/A
SC3a	50
SC3b	50
SC4	N/A
SC4a	N/A
SC4b	N/A
SC5	N/A

Table 13: Number of hazards per Severity Class per Accident Type (MAC CFIT)

With the defined number of hazards per Severity Class per Accident Type and the Severity Class Schemes for CFIT - AIM CFIT Barrier Model (Figure 1) below the overall number of operational hazards for the given severity class at any given barrier can be determined. The Severity Class Scheme shows a simplified version of the corresponding Accident Incident Models.

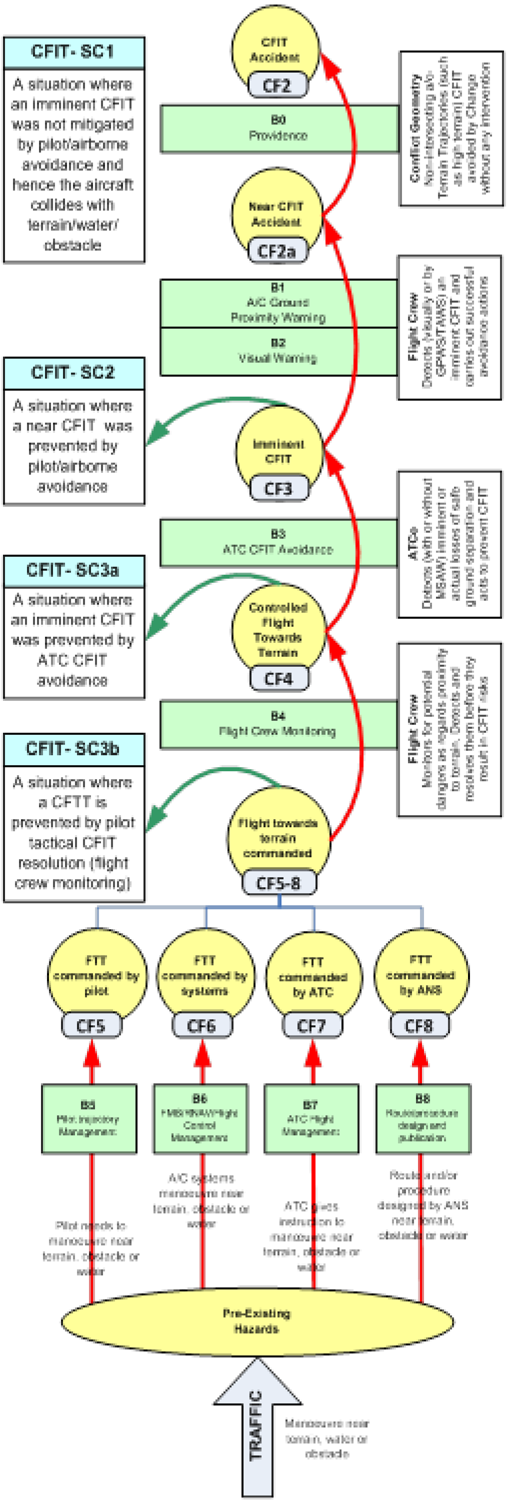


Figure 1: Severity Class Scheme for CFIT - AIM CFIT Barrier Model

Table 14 shows the Risk Classification Scheme for CFIT. For each of the four given Severity Classes the hazardous situation and the corresponding operational effect are explained. The Maximum Tolerable Frequency of Occurrence (MTFoO) per flight hour for these Severity Classes can also read off from the table and used to calculate the allowable frequency for the different CFIT-related Safety Objectives with the given formula.

Severity Class	Hazardous situation	Operational Effect	MTFoO [per fh]
CFIT-SC1	A situation where an imminent CFIT is not mitigated by pilot/airborne avoidance and hence the aircraft collides with terrain/water/obstacle	CFIT Accident (CF2) Near CFIT (CF2a)	1e-8
CFIT-SC2	A situation where a near CFIT is prevented by pilot/airborne avoidance	Imminent CFIT (CF3)	1e-6
CFIT-SC3a	A situation where an imminent CFIT is prevented by ATC CFIT avoidance	Controlled flight towards terrain (CF4)	1e-5
CFIT-SC3b	A situation where a controlled flight towards terrain is prevented by pilot tactical CFIT resolution (flight crew monitoring)	Flight towards terrain commanded (CF5-8)	1e-5

Table 14: Risk Classification Scheme for CFIT

Table 15 lists Safety Objectives (integrity/reliability) for the identified hazards calculated as described above.

ID	Safety Objectives
Hz-001	SO-0101: Frequency of occurrence of helicopter deviating laterally or vertically from advanced PinS towards terrain in controlled airspace leading to CFTT shall not be greater than 2x10-7/flight.

Table 15: Safety Objectives (integrity/reliability)

3.9 Impacts of PJ.01-06 Solution operations on adjacent airspace or on neighbouring ATM Systems

The new procedure does not have any direct impact on safety of adjacent sectors or neighbouring ATM Systems.

3.10 Achievability of the Safety Criteria

Table 16 shows the achievability of the Safety Criteria set in Section 3.5, which are achieved through the specification of safety objectives (functionality, performance and integrity).

Safety Criteria	Safety Objectives
SAC101: The number of Controlled Flight	SO-0001

Towards Terrain (CF4) shall remain the new concept.	
SAC102: The number of Flight Towards Terrain Commanded by Pilot (CF5) shall be reduced by the new concept due to the use of an HMD.	SO-0002 SO-0004 SO-0005 SO-0006 SO-0007
SAC103: The number of Flight Towards Terrain Commanded by System (CF5) shall remain with the new concept.	SO-0003 SO-0006 SO-0007 SO-0101

Table 16: Achievability of the Safety Criteria

3.11 Validation & Verification of the Safety Specification

Results of the Safety Analysis by the different exercises can be found in PJ.01-06 V3 VALR.

4 Safe Design at SPR Level

4.1 Scope

This section addresses the following activities:

- Description of the Functional Model (see Guidance G.1.2 of [2]) of the end-to-end Solution ATM System – section 4.2 (it is optional as to whether the safety assessor uses a functional model or goes straight to the SPR-level model; in the latter case, delete section 0).
- Description of the SPR-level model (see Guidance G.2 of [2]) of the end-to-end Solution ATM System - section 4.3
- Derivation, from the Safety Objectives (Functionality and Performance) of section 3, of Safety Requirements for the SPR-level design - section 4.3
- Analysis of the operation of the SPR-level design under normal operational conditions – section 0
- Analysis of the operation of the SPR-level design under abnormal conditions of the Operational Environment - section 4.5
- Assessment of the adequacy of the SPR-level design in the case of internal failures and mitigation of the System-generated hazards - section 4.6
- Justification that the SAfety Criteria are capable of being satisfied in a typical implementation - section 4.7
- Realism of the SPR-level design - section 4.8
- Validation & verification of the Specification - section 4.9”

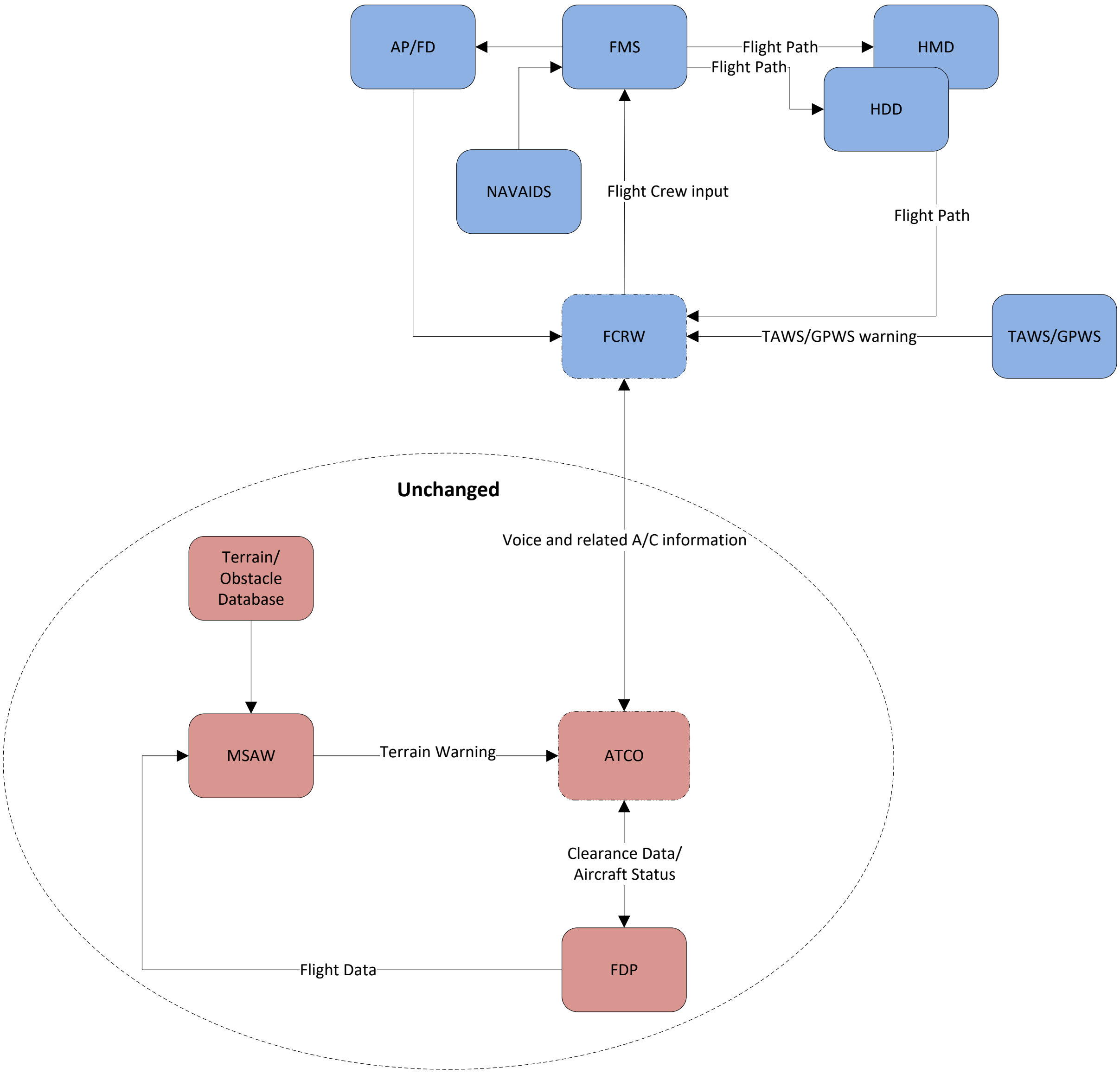
4.2 The PJ.01-06 Solution Functional Model

Not applicable see chapter 4.1

4.3 The PJ.01-06 Solution SPR-level Model

In this Chapter the SPR-level Model is described. This model is a high-level architectural representation of the Solution System. The Model describes the main human tasks, ground equipment functions and airspace design of the Flight Centric Solution. Human-machine interfaces are not shown explicitly on the model to avoid unnecessary complexity.

4.3.1 Description of SPR-level Model



The symbols used in the model are as follows (box titles are illustrative):

Flight Centric Controller 1	Human actor – ground
Medium Term Conflict Detection System	Equipment – ground
FCRW	Human actor – airborne

FMS	Equipment – airborne
→	Main interface

The Acronyms used in the SPR-level Model are as follows:

AP	Autopilot
ATCO	Air Traffic Controller
FCRW	Flight Crew
FD	Flight Director
FDP	Flight Data Processor
FMS	Flight Management System
GPWS	Ground Proximity Warning System
HDD	Head-Down Display
HMD	Head-Mounted Display
MSAW	Minimum Safe Altitude Warning
NAVAIDS	Navigation system and supporting NAVAIDS
TAWS	Terrain awareness and warning system

4.3.1.1 Aircraft Elements

- AP (Autopilot): An autopilot is a device used to guide an aircraft without direct assistance from the pilot. Early autopilots were only able to maintain a constant heading and altitude, but modern autopilots are capable of controlling every part of the flight envelope from just after take-off to landing. Modern autopilots are normally integrated with the flight management system (FMS) and, when fitted, the auto throttle system [7]. Autopilot is needed to fly RF-legs in normal operations.

- FCRW (Flight Crew): The Flight Crew in the SPR level model represents the aircraft which is controlled by the Air Traffic Controller. The Flight Crew is impacted due to the advanced PinS procedures (e.g. contingency procedures).

- FD (Flight Director): The flight director computes and displays the proper pitch and bank angles required in order for the aircraft to follow a selected path. Flight director guidance can be used in both manual flight and with the Autopilot engaged. [7].

- FMS (Flight Management System): A Flight Management System (FMS) is an on-board multi-purpose navigation, performance, and aircraft operations computer designed to provide virtual data and operational harmony between closed and open elements associated with a flight from pre-engine start and take-off, to landing and engine shut-down. [7] The FMS is impacted due to the advanced PinS procedures (RNP 0.3 required/ RF required).
- GPWS (Ground Proximity Warning System): The Ground Proximity Warning System (GPWS) generates advisory Alerts and mandatory response Warnings to the flight crew in respect of their proximity to terrain. [7] Ground Proximity Warning System is not impacted by the advanced PinS procedures.
- HDD (Head-down display): The Head-Down Display means the normal displays in the cockpit such as speed indicator, altimeter and bank indicator.
- HMD (Head-Mounted Display): A HMD is a helmet with an integrated display which supports the pilot with important information such as the flight path. Head-Mounted Display is optional for advanced PinS procedures.
- TAWS (Terrain awareness and warning system): A system that provides the flight crew with sufficient information and alerting to detect a potentially hazardous terrain situation and so the Flight Crew may take effective action to prevent a CFIT event. [7] Terrain awareness and warning system is not impacted by the advanced PinS procedures.

4.3.1.2 Ground Elements

- ATCO (Air Traffic Controller): The Air Traffic Controller is responsible for all rotorcraft/aircraft in his sector.
- FDP (Flight Data Processor): The Flight Data Processor receives all clearance data provided by the ATCO.
- MSAW (Minimum Safe Altitude Warning): A ground-based safety net intended to warn the controller about increased risk of controlled flight into terrain accidents by generating, in a timely manner, an alert of aircraft proximity to terrain or obstacles. [7]

4.3.1.3 External Entities

N/A

4.3.2 Task Analysis

An analysis of the controller tasks can be found in PJ.01-06 V3 SPR-INTEROP/OSED Part IV.

Derivation of Safety Requirements (Functionality and Performance – success approach)Table 17 lists the Safety Objectives (Functionality and Performance – success approach) and the corresponding Safety Requirements as well as their representation in the SPR-level model.

Safety Objectives (Functionality and Performance from success approach)	Requirement (forward reference)	Maps on to

SO-0001 FCRW monitoring during A-PinS operation shall be effective.	SR-1001 FCRW shall be able to detect lateral route deviation greater than 0.3Nm including during RF leg using HDD or HMD	HDD - HMD
	SR-1002 FCRW shall be able to detect lateral and vertical route deviation during final LPV approach using HDD or HMD	HDD - HMD
SO-0002 Trajectory management by FCRW shall be effective during A-PinS operation.	SR-1003 The HMD symbology shall help the pilot to control laterally and vertically the trajectory and shall indicate the flight parameters (speed, altitude, velocity vector…) at any time	HMD
SO-0003 Trajectory management by A/C systems shall be effective during A-PinS operation	SR-1004 RNP system shall be approved in accordance with the RNP 0.3 navigation specification	FMS
	SR-1005 FMS system shall be approved for RNP approach down to LPV minima	FMS
	SR-1006 RNP system coupled with AP /FD shall be capable of executing RF legs	FMS
	SR-1007 The FMS shall provide advanced PinS guidance during the curved segment between the Intermediate Fix and the Final Approach Fix, which combines longitudinal, lateral and vertical movements.	FMS

Table 17: Mapping of Safety Objectives to SPR-level Model Elements

Table 18 lists the Safety Requirements (Functionality and Performance – success approach) and the corresponding Safety Objectives

Safety Requirement (functionality & performance) [SPR-level Model Element]	Requirement	Derived from Table 18
SR-1001	FCRW shall be able to detect lateral route deviation greater than 0.3Nm including during RF leg using HDD or HMD	SO-0001
SR-1002	FCRW shall be able to detect lateral and vertical route deviation during final LPV approach using HDD or HMD	SO-0001
SR-1003	The HMD symbology shall help the pilot to control laterally and vertically the trajectory and shall indicate the flight parameters (speed, altitude, velocity vector…) at any time	SO-0002
SR-1004	RNP system shall be approved in accordance with the RNP 0.3 navigation specification	SO-0003
SR-1005	FMS system shall be approved for RNP approach down to LPV minima	SO-0003
SR-1006	RNP system coupled with AP /FD shall be capable of executing RF legs	SO-0003
SR-1007	The FMS shall provide advanced PinS guidance during the curved segment between the Intermediate Fix and the Final Approach Fix, which combines longitudinal, lateral and vertical movements.	SO-0003

Table 18: Derivation of Safety Requirements (functionality and performance) from Safety Objectives

4.3.3 Traceability

It was decided to start with the creation of a SPR-level model. Hence there is no traceability between FM-level model and SPR-level model in this document (see section 4.1)

4.4 Analysis of the SPR-level Model – Normal Operational Conditions

This section is concerned with ensuring that the SPR-level design is complete, correct and internally coherent with respect to the Safety Requirements (success approach) derived for the normal operating conditions that were used to develop the corresponding Safety Objectives (success approach) in section 3.6.2

The analysis necessarily depends on proving the Safety Requirements (Functionality and Performance) from three perspectives:

- a static view of the System behaviour using a Thread Analysis technique, as described in sections 4.4.2 and 4.4.3 for the scenarios for normal operations described in section 4.4.1 (from the Solution SPR-INTEROP/OSED)
- check that the System design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets, through static analysis and simulation - see section 4.4.4
- a dynamic view of the System behaviour using in particular Real-time simulations - see section 4.4.5

4.4.1 Scenarios for Normal Operations

Table 19 list the operational scenarios for normal operations as described in the PJ.01-06 V3 SPR-INTEROP/OSED

ID	Scenario	Rationale for the Choice
1	Use Case 1: Departure PinS procedure	Use Case Analysis (see SPR-INTEROP/OSED Part I, Chapter 3.3.2.1.1.1.1)
2	Use Case 2: Approach PinS procedure	Use Case Analysis (see SPR-INTEROP/OSED Part I, Chapter 3.3.2.1.1.1.2)

Table 19: Operational Scenarios – Normal Conditions

4.4.2 Thread Analysis of the SPR-level Model – Normal Operations

4.4.2.1 Scenario # 1

This Use Case describes a departure with PinS procedure.

Preconditions

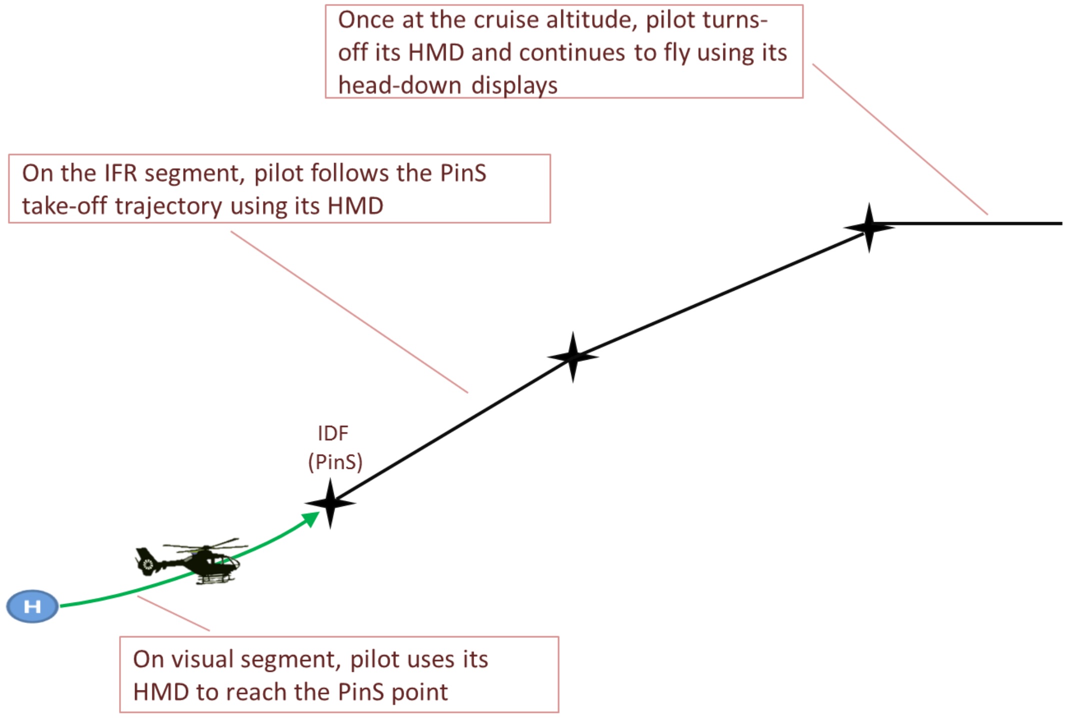
Flight is going to depart at an airport.

Postconditions: Success end state

Flight is departed and handed-over to the En-Route Controller

Main Flow
1. Visual flight with HMD to the first point of the instrument procedure, the IDF (Initial Departure Fix)
2. On IFR segment, pilot follows the PinS take-off trajectory using HMD

3. Once cruise altitude has been reached, pilot can turn-off HMD and continue a normal instrument flight using head-down displays.



PinS departure using HMD – Vertical profile

4.4.2.2 Scenario # 2

This Use Case describes an arrival with PinS procedure.

Preconditions

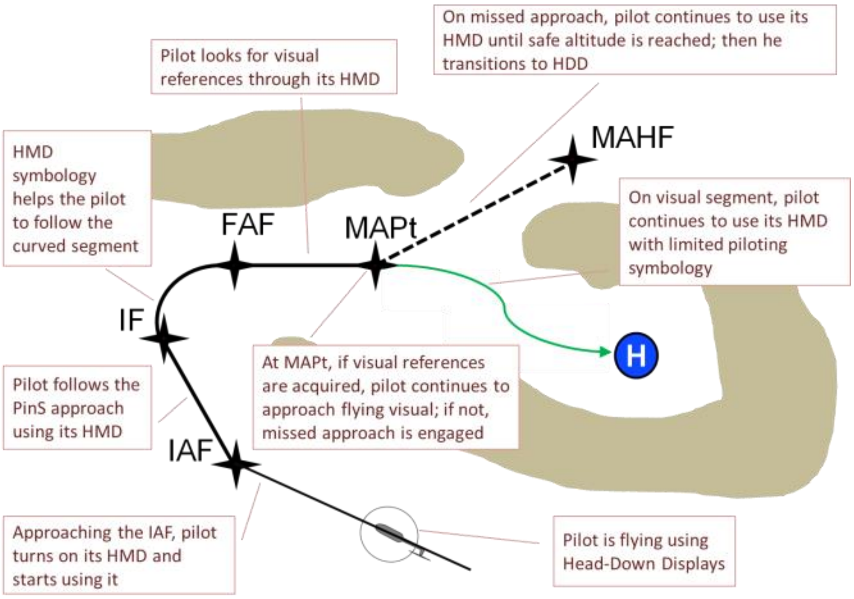
Flight is going to arrive at an airport.

Postconditions: Success end state

Flight is arrived at the airport

Main Flow
1. Flight using Head-Down Display until reaching IAF
2. At Initial Approach Fix (IAF) pilot turns on the HMD. HMD symbology helps pilot to follow curved segment.
3. Between FAF and MAPt pilot looks for visual references through HMD.
4. At MAPt, if visual references are acquired, pilot continues to approach flying visual.

5. On visual segment, pilot continues to use HMD with limited piloting symbology.



PinS approach using HMD – Lateral profile

4.4.3 Effects on Safety Nets – Normal Operational Conditions

The described normal operating conditions do not affect existing safety nets. In addition, the new process does not require any additional "new" safety nets.

4.4.4 Dynamic Analysis of the SPR-level Model – Normal Operational Conditions

N/A

4.4.5 Additional Safety Requirements (functionality and performance) – Normal Operational Conditions

No additional safety requirements have been revealed by the above analyses.

4.5 Analysis of the SPR-level Model – Abnormal Operational Conditions

This section is concerned with ensuring that the SPR-level Design is complete, correct and internally coherent with respect to the Safety Requirements (Functionality and Performance) derived for the abnormal operating conditions that were used to derive the corresponding Safety Objectives (success approach) in section 3.6.2

The analysis should be carried out from three perspectives:

- can the Solution ATM System continue to operate effectively – i.e. reduce risk?

- if the Solution ATM System cannot continue to operate fully effectively – i.e. its risk reduction performance is diminished somewhat – is the overall risk still within the tolerable limits and can the System recover sufficiently quickly when the abnormality is removed (or at least mitigated)
- to what degree could such abnormal conditions, while they persist, cause the Solution ATM System to behave in a way that could actually induce a risk that would otherwise not have arisen?

4.5.1 Scenarios for Abnormal Conditions

Table 20 lists the abnormal operational scenarios as described in PJ.01-06 V3 SPR-INTEROP/OSED

ID	Scenario	Rationale for the Choice
	Advanced PinS operation without GNSS/SBAS	Use Case Analysis (see SPR-INTEROP/OSED Part I, Chapter 3.3.2.1.1.1.2)
	Approach PinS procedure with missed approach due to adverse weather conditions	Use Case Analysis (see SPR-INTEROP/OSED Part I, Chapter 3.3.2.1.1.1.2)

Table 20: Operational Scenarios – Abnormal Conditions

Derivation of Safety Requirements (Functionality and Performance) for Abnormal ConditionsTable 21 lists the abnormal conditions defined with the corresponding Safety Objectives (Functionality and Performance) to mitigate the consequences of the abnormal conditions as well as the corresponding Safety Requirements (Functionality and Performance).

Ref	Abnormal Conditions / SO (*Functionality and Performance)*	Mitigations (SR 0xx and/or A 0xx)
1	SO-0004 FCRW shall revert to contingency procedures in case of loss of GNSS during advanced PinS operation	SR-1008 Helicopter operator shall define contingency procedure in case of loss of GNSS and/or SBAS during A-PinS operations and considering local environment
		SR-1009 In case of loss of GNSS and/or SBAS during PinS operation, FCRW shall respect helicopter operator's contingency procedures (e,g, conventional navigation or dead reckoning)
		SR-1010 The status of GNSS/SBAS (vertical guidance) shall be displayed to the FCRW at any time

2	SO-0005 FCRW shall be supported by HMD in case of DVE	SR-1011 The HMD shall visually provide all relevant data when approaching the missed approach point to support the FCRW in the decision whether to continue or abort the approach procedure

Table 21: Safety Requirements or Assumptions to mitigate abnormal conditions

4.5.2 Thread Analysis of the SPR-level Model - Abnormal Conditions

4.5.2.1 Scenario # 1

This Use Case describes an arrival with PinS procedure.

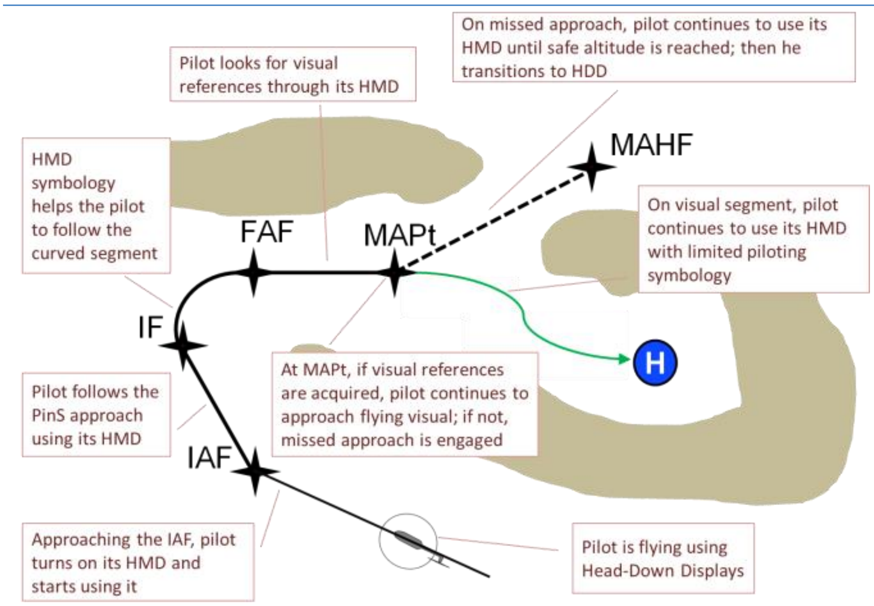
Preconditions

Flight is going to arrive at an airport.

Postconditions

Missed approach procedure due to adverse weather.

Main Flow
1. Flight using Head-Down Display until reaching IAF.
2. At Initial Approach Fix (IAF) pilot turns on the HMD. HMD symbology helps pilot to follow curved segment.
3. Between FAF and MAPt pilot looks for visual references through HMD.
4. At MAPt, if visual references not acquired, pilot flies missed approach procedure.
5. On missed approach, pilot continues to use its HMD until safe altitude is reached.
6. Transition to HDD.



PinS approach using HMD – Lateral profile

4.5.3 Effects on Safety Nets – Abnormal Operational Conditions

The described abnormal operating conditions do not affect existing safety nets. In addition, the new process does not require any additional "new" safety nets.

4.5.4 Dynamic Analysis of the SPR-level Model – Abnormal Operational Conditions

Results of the Safety Analysis by the different exercises can be found in PJ.01-06 V3 VALR.

4.5.5 Additional Safety Requirements – Abnormal Operational Conditions

No additional Safety Requirements from Thread Analysis for Abnormal Operating Conditions have been revealed.

4.6 Design Analysis – Case of Internal System Failures

Since the consequences of the identified System-generated hazards were derived and analysed (at the OSED level) in the FHA process of section 3.8 above, this part of the safety assessment focuses on the causes of those hazards. This is done in 7 steps, as follows:

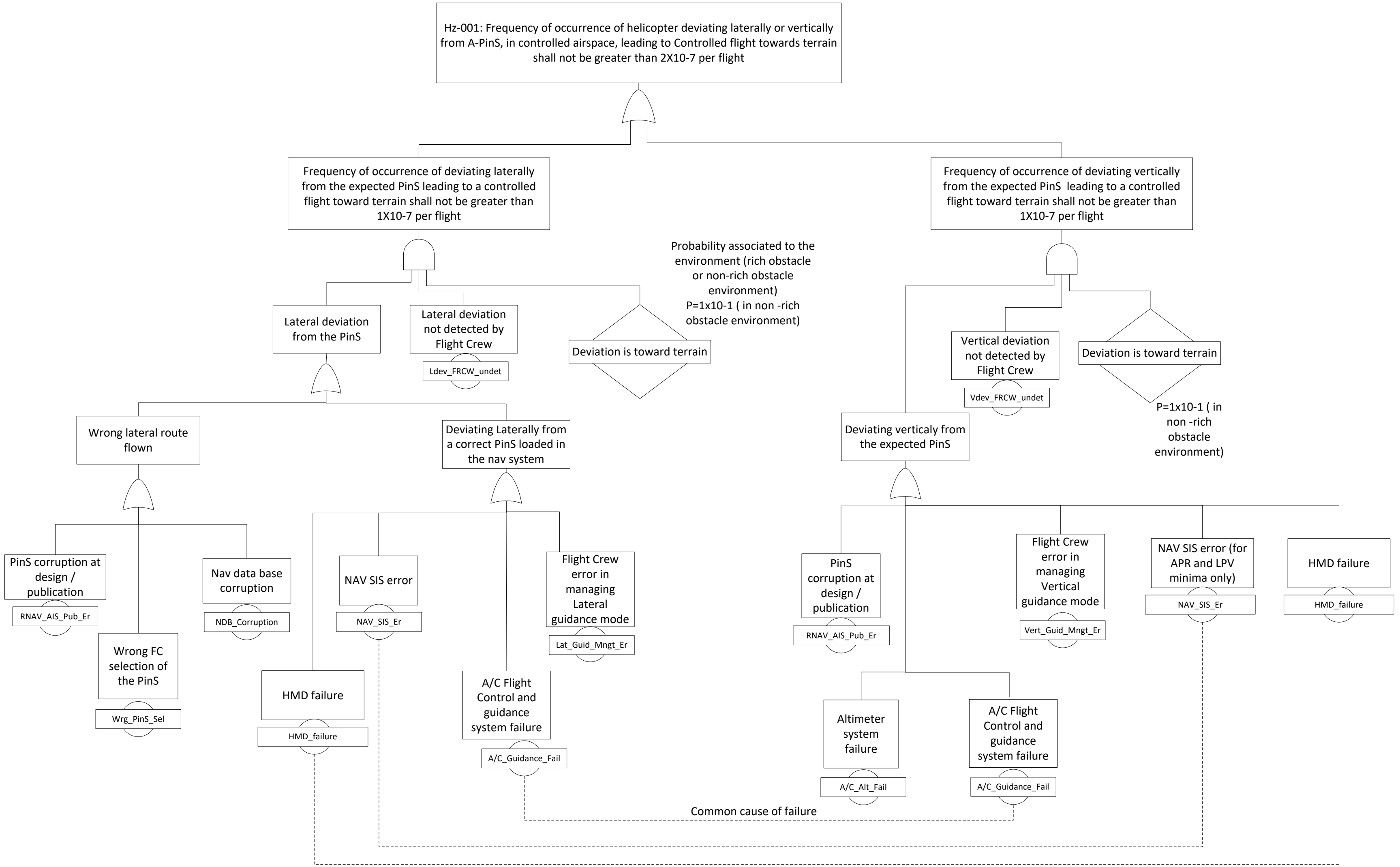
1. For each System-generated hazard, top-down identification of internal System failures that could cause the hazard
2. Assessment (bottom-up) of the consequences of failure for each System element / element-to-element interface - i.e. common-cause analysis
3. Derivation of mitigations to reduce the likelihood that specific failures would propagate up to the Hazard (i.e. operational level) - these mitigations are then captured as additional Safety Requirements (Functionality and Performance)
4. Demonstration of the completeness of the mitigating Safety Requirements
5. Demonstration of the feasibility and effectiveness of the associated System reversionary modes
6. Setting of Safety Requirements to limit the frequency with which each identified System failure could be allowed to occur, taking into account the mitigations above
7. Analysing whether the Safety Requirements (integrity/reliability) are achievable

For these steps the following methods were used:

- Fault Tree Analysis (steps 1, 3 and 6)
- Failure Modes, Effects and Criticality Analysis (step 2)
- Static analysis (step 4)
- Simulations (step 5)
- Human Reliability Assessment (step 7).

4.6.1 Causal Analysis

In the following the Fault-Tree for the Hazard (Hz-001) defined in Chapter 3.8.1 is shown.



Hz-001: Frequency of occurrence of helicopter deviating laterally or vertically from A-PinS, in controlled airspace, leading to Controlled flight towards terrain shall not be greater than 2X10-7 per flight
Frequency of occurrence of deviating laterally from the expected PinS leading to a controlled flight toward terrain shall not be greater than 1X10-7 per flight
Frequency of occurrence of deviating vertically from the expected PinS leading to a controlled flight toward terrain shall not be greater than 1X10-7 per flight
Probability associated to the environment (rich obstacle or non-rich obstacle environment) P=1x10-1 (in non -rich obstacle environment)
Lateral deviation from the PinS
Lateral deviation not detected by Flight Crew
Ldev_FRCW_undet
Deviation is toward terrain
Vertical deviation not detected by Flight Crew
Vdev_FRCW_undet
Deviation is toward terrain
P=1x10-1 (in non -rich obstacle environment)
Wrong lateral route flown
Deviating Laterally from a correct PinS loaded in the nav system
Deviating verticaly from the expected PinS
PinS corruption at design / publication
RNAV_AIS_Pub_Er
Nav data base corruption
NDB_Corruption
NAV SIS error
NAV_SIS_Er
Flight Crew error in managing Lateral guidance mode
Lat_Guid_Mngt_Er
PinS corruption at design / publication
RNAV_AIS_Pub_Er
Flight Crew error in managing Vertical guidance mode
Vert_Guid_Mngt_Er
NAV SIS error (for APR and LPV minima only)
NAV_SIS_Er
HMD failure
HMD_failure
Wrong FC selection of the PinS
Wrg_PinS_Sel
HMD failure
HMD_failure
A/C Flight Control and guidance system failure
A/C_Guidance_Fail
Altimeter system failure
A/C_Alt_Fail
A/C Flight Control and guidance system failure
A/C_Guidance_Fail
Common cause of failure

Figure 2: Hz-001 Loss of GNSS signal during PinS operation

4.6.2 Common Cause Analysis

In the following the consequences of failure for each System element / element-to-element interface are analysed for each identified hazard and new Safety Requirements and Assumptions are defined.

Hz-001 Basic Causes [SPR-level Model Element]	Failure Cause description	Requirement / Assumption
Ldev_FRCW_undet	A lateral deviation is not detected by FCRW.	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
Vdev_FRCW_undet	A vertical deviation is not detected by FCRW.	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
RNAV_AIS_Pub_Er	The design / publication of advanced PinS procedure is false.	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
Wrg_PinS_Sel	The Flight Crew selects wrong advanced PinS procedure in the FMS:	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
NDB_Corruption	The Navigation data base is false (e.g. old version)	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
HMD_failure	Head-Mounted Display does not work properly.	SR-1012 Helicopter operator shall define contingency procedure in case of loss of HMD during advanced PinS operations and considering local environment SR-1013 In case of loss of HMD during PinS operation, FCRW shall respect helicopter operator's contingency procedures.

		SR-1014 The status of HMD (vertical guidance) shall be displayed to the FCRW at any time SR-1101 HMD data corruption shall occur less than 1*10-7.
NAV_SIS_Er	NAV SIS failure	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
A/C_Guidance_Fail	A/C Flight Control and guidance system failure	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
Lat_Guid_Mngt_Er	Flight Crew error in managing Lateral guidance mode	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
A/C_Alt_Fail	Altimeter system failure	Changes due to the advanced PinS procedure compared to standard PinS are not expected.
Vert_Guid_Mngt_Er	Flight Crew error in managing Vertical guidance mode	Changes due to the advanced PinS procedure compared to standard PinS are not expected.

Table 22: Hazard-Analysis - Hz-001

4.6.3 Formalization of Mitigations

Table 23 lists the Safety Objectives (Functionality and Performance – failure approach) and the corresponding Safety Requirements as well as their representation in the SPR-level model.

Safety Objectives **(Functionality and Performance from failure approach)**	**Requirement** **(forward reference)**	**Maps on to**
SO-0006 FCRW shall revert to contingency procedures in case of loss of HMD during Advanced PinS operation.	SR-1012 Helicopter operator shall define contingency procedure in case of loss of HMD during advanced PinS operations and considering local environment SR-1013 In case of loss of HMD during PinS operation, FCRW shall respect helicopter operator's contingency procedures. SR-1014 The status of HMD (vertical guidance) shall be displayed to the FCRW at any time	HMD
SO-0007 FCRW shall revert to contingency procedures in case of loss of AP during advanced PinS operation.	SR-1015 Helicopter operator shall define contingency procedure in case of loss of AP during advanced PinS operations and considering local environment SR-1016 In case of loss of AP during PinS operation, FCRW shall respect helicopter operator's contingency procedures	AP

Table 23: Mapping of Safety Objectives failure approach to SPR-level Model ElementsTable 24 lists the Safety Requirements (Functionality and Performance – success approach) and the corresponding Safety Objectives.

Safety Requirement **(functionality & performance)**	**Requirement**	**Derived from Table 23**

[SPR-level Model Element]		
SR-1012	Helicopter operator shall define contingency procedure in case of loss of HMD during A-PinS operations and considering local environment	SO-0006
SR-1013	In case of loss of HMD during PinS operation, FCRW shall respect helicopter operator's contingency procedures	SO-0006
SR-1014	The status of HMD shall be displayed to the rotorcraft pilot at any time.	SO-0006
SR-1015	Helicopter operator shall define contingency procedure in case of loss of AP during A-PinS operations and considering local environment	SO-0007
SR-1016	In case of loss of AP during PinS operation, FCRW shall respect helicopter operator's contingency procedures	SO-0007

Table 24: Derivation of Safety Requirements (functionality and performance from failure approach) from Safety Objectives

4.6.4 Safety Requirements (integrity/reliability)

Table 25 lists the Safety Objectives (integrity and reliability – failure approach) and the corresponding Safety Requirements as well as their representation in the SPR-level model.

Safety Objectives (Integrity and reliability from failure approach)	Requirement (forward reference)	Maps on to
SO-0101 Frequency of occurrence of helicopter deviating laterally or vertically from A-PinS towards terrain in controlled airspace leading to CFTT shall not be greater than 2x10-7/flight.	SR-1101 HMD data corruption shall occur less than 1*10-7.	HMD

Table 25: Mapping of Safety Objectives (Integrity and reliability from failure approach) to SPR-level Model Elements

Table 26 lists the Safety Requirements (Integrity and Reliability – success approach) and the corresponding Safety Objectives.

Safety Requirement (Integrity and reliability from	Requirement	Derived from Table 25

failure approach) **[SPR-level Model Element]**		
SR-1101	HMD data corruption shall occur less than 1*10-7.	SO-0101

Table 26: Derivation of Safety Requirements (integrity and reliability from failure approach) from Safety Objectives

4.7 Achievability of the Safety Criteria

Table 27 shows the achievability of the Safety Criteria set in Section 3.5, which are achieved through the specification of safety requirements (functionality, performance and integrity).

Safety Criteria	Safety Requirements
SAC101: The number of Controlled Flight Towards Terrain (CF4) shall remain the new concept.	SR-1001 SR-1002
SAC102: The number of Flight Towards Terrain Commanded by Pilot (CF5) shall be reduced by the new concept due to the use of an HMD.	SR-1003 SR-1008 SR-1009 SR-1010 SR-1011 SR-1012 SR-1013 SR-1014 SR-1015 SR-1016
SAC103: The number of Flight Towards Terrain Commanded by System (CF5) shall remain with the new concept.	SR-1004 SR-1005 SR-1006 SR-1007 SR-1012 SR-1013

	SR-1014 SR-1015 SR-1016 SR-1101

Table 27: Achievability of the Safety Criteria

4.8 Realism of the SPR-level Design

4.8.1 Achievability of Safety Requirements / Assumptions

All defined Safety Requirements are achievable (Expert judgement).

4.8.2 "Testability" of Safety Requirements

All defined Safety Requirements are testable (Expert judgement).

4.9 Validation & Verification of the Safe Design at SPR Level

Results of the Safety Analysis by the different exercises can be found in PJ.01-06 V3 VALR.

5 Acronyms and Terminology

Term	Definition	Source of the definition
ADS-B Application	A means by which aircraft, can automatically transmit and/or receive data such as identification, position and additional data, as appropriate, in a broadcast mode via a data link.	ICAO Documentation
Airspace Management	Airspace Management is the process by which airspace options are selected and applied to meet the needs of the ATM community.	ICAO 9854
	Airspace Management is integrated with Demand and Capacity Balancing activities and aims to define, in an inclusive, synchronised and flexible way, an optimised airspace configuration that is relevant for local, sub-regional and regional level activity to meet users requirements in line with relevant performance metrics. Airspace Management primary objective is to optimise the use of available airspace, in response to the users demands, by dynamic time-sharing and, at times, by the segregation of airspace among various airspace users on the basis of short-term needs. It aims at defining and refining, in a synchronised and a flexible way, the most optimum airspace configuration at local, sub-regional and regional levels in a given airspace volume and within a particular timeframe, to meet users requirements while ensuring the most performance of the European Network and avoiding as much as possible any disruption. Airspace Management in conjunction with AFUA is an enabler to improve civil-military co-operation and to increase capacity for the benefit of all users.	P07.02 P04.02
Airspace Configuration:	Is a pre-defined and coordinated organisation of ATS routes of the ARN and /or terminal routes and their associated airspace structures, including airspace reservations/restrictions (ARES), if appropriate, and ATC sectorisation.	OSED 07.05.02 AFUA Step 1 V3 for V4

Airspace Restriction	A defined volume of airspace within which, variously, activities dangerous to the flight of aircraft may be conducted at specified times (a "danger area"); or such airspace situated above the land areas or territorial waters of a State, within which the flight of aircraft is restricted in accordance with certain specified conditions (a restricted area); or airspace situated above the land areas or territorial waters of a State, within which the flight of aircraft is prohibited (a prohibited area).	OSED 07.05.02 Step 1 V" for V4
Airspace Structure	A specific volume of airspace designed to ensure the safe and optimal operation of aircraft.	OSED 07.05.02 Step 1 AFUA V3 for V4
Area navigation (RNAV)	Method of navigation which permits aircraft operation on any desired flight path within the coverage of station-referenced navigation aids or within the limits of the capability of self-contained aids, or a combination of these. Note.— Area navigation includes performance-based navigation as well as other RNAV operations that do not meet the definition of performance-based navigation	ICAO Doc 9613 PBN Manual
Approach procedure with vertical guidance (APV)	An instrument procedure which utilizes lateral and vertical guidance but does not meet the requirements established for precision approach and landing operations. These procedures are enabled by GNSS and Baro VNAV or by SBAS. (PBN).	ICAO Documentation
APV Baro-VNAV	RNP APCH down to LNAV/VNAV minima.	ICAO Documentation
APV SBAS	RNP APCH down to LPV minima.	ICAO Documentation
Baro-VNAV	Barometric vertical navigation (Baro-VNAV) is a navigation system that presents to the pilot computed vertical guidance referenced to a specified vertical path angle (VPA), nominally 3°. The computer-resolved vertical guidance is based on barometric altitude and is specified as a VPA from reference datum height (RDH). (PANS OPS).	ICAO Documentation
CDFA – Continuous Descent Final Approach	Continuous Descent Final Approach is a technique for flying the final approach segment of an NPA as a continuous descent. The technique is consistent with stabilized approach procedures and has no level-off. A CDFA starts from an altitude/height at	ICAO Documentation

	or above the FAF and proceeds to an altitude/height approximately 50 feet (15 meters) above the landing runway threshold or to a point where the flare manoeuvre should begin for the type of aircraft being flown. This definition is harmonized with the ICAO and the European Aviation Safety Agency (EASA).	
Flight intent	The future aircraft trajectory expressed as a 4-D profile up to the destination (taking into account of aircraft performance, weather, terrain, and ATM service constraints). It is calculated and “owned” by the aircraft flight management system, and agreed by the Pilot.	ICAO Doc 9854
	In the SESAR Context, Flight Intent corresponds to the "agreed data of RB/MT” : the waypoints of the routes and associated altitude, possible time and/or speed constraints agreed between ATM actors.	WP B04.02 CONOPS Step 1
Final Approach Point/Fix (FAP/FAF)	In PANS-OPS ICAO Doc 8168 VOL I, FAF is described as the beginning of the final approach segment of an Non-Precision Approach, and FAP is described as the beginning of the final approach segment of a Precision Approach. Moreover, PANS-OPS ICAO Doc 8168 VOL II states that the APV segment of an APV SBAS procedure starts at the Final Approach Point. So, within this document, since only APV SBAS procedures are considered, the beginning of the final approach segment is called the FAP	PANS-OPS ICAO Doc 8168 VOL I
Final Approach Segment (FAS) Data Block	The APV database for SBAS includes a FAS Data Block. The FAS Data Block information is protected with high integrity using a cyclic redundancy check (CRC).	PANS OPS
GNSS – Global Navigation Satellite System	A worldwide position and time determination system that includes one or more satellite constellations, aircraft receivers and system integrity monitoring, augmented as necessary to support the required navigation performance for the intended operation.	ICAO Annex 10
Low Level IFR Routes	Low Level IFR Routes dedicated to Rotorcraft integration in dense / constrained airspace. Rotorcraft altitude (2000-4000 ft.) specific Low Level IFR routes are designed and optimised	ICAO Documentation

	based on route network using RNP-1 / RNP-0.3. The integration in dense and constraint airspace TMA is due to rotorcraft peculiar flight characteristics and type of operation conducted, such as: • Helicopters not pressurised: the Maximum allowed altitude: FL100 (e.g 3000 m) • Most helicopters have no de-icing capability • Risk of encountering icing conditions increases with altitude. Typically standard IFR FL are often too high • Health of on-board patients during medical flights • Recommended altitude for patients in critical condition: not more than 3000 ft. AGL • Safety and environment • Visual flight at very low height (500 ft. or sometimes less) to stay below clouds in marginal weather conditions is frequent accident cause and impacts environment (e.g noise footprint)	
LNAV, LNAV/VNAV, LPV	Are different levels of approach service and are used to distinguish the various minima lines on the RNAV (GNSS) chart. The minima line to be used depends on the aircraft capability and approval.	ICAO Documentation
LNAV/VNAV	The minima line based on Baro-VNAV system performances that can be used by aircraft approved according to AMC 20-27 or equivalent. LNAV/VNAV minima can also be used by SBAS capable aircraft according to CM-AS-002 Issue 2.	ICAO Documentation
LPV (Localiser Performance with Vertical Guidance)	The minima-line based on SBAS performances that can be used by aircraft approved according to AMC 20-28 or equivalent	ICAO Documentation
MAPt	Missed Approach Point	ICAO Documentation
Navigation specification	A navigation specification is a set of aircraft and aircrew requirements needed to support a navigation application within a defined airspace concept.	ICAO Doc 9613 and WP B04.02 CONOPS Step 1

	The navigation specification: • defines the performance required by the navigation system, • prescribes the performance requirements in terms of accuracy, integrity, continuity and availability for proposed operations in a particular Airspace, • also describes how these performance requirements are to be achieved i.e. which navigation functionalities are required to achieve the prescribed performance and associated requirements related to pilot knowledge and training and operational approval. A Performance-Based Navigation Specification is either a RNAV specification or a RNP specification. RNAV specifies a required accuracy whilst RNP specifies, in addition to a required accuracy, an aircraft system alert in case of deviation, with the pilot responsible to remain the aircraft within the RNP accuracy; it allows reducing ATC buffer with the controller still responsible for the separation against traffic.	
Network Management	Network Management is an integrated activity with the aim of ensuring optimised Network Operations and ATM service provision meeting the Network performance targets., The Network Management Function is executed at all levels (Regional, Sub-regional and Local) throughout all planning and execution phases, involving, as appropriate, the adequate actors (NM, FM, LTM…)	P07.02 P04.02
Performance-Based Navigation (PBN)	Area navigation based on performance requirements for aircraft operating along an ATS route, on an instrument approach procedure or in a designated airspace. *Note.— Performance requirements are expressed in navigation specifications in terms of accuracy, integrity,* *continuity, availability and functionality needed for the proposed operation in the context of a*	ICAO DOC 9613 PBN Manual

	particular airspace concept	
PinS	Point in Space is an RNP approach procedure designed for helicopters only that includes both a visual and an instrument segment Two types of PinS are defined in this document. These terms are not listed in ICAO PANS-OPS. - standard PinS: straight in PinS RNP APCH down to LPV or LNAV minima - advanced PinS: PinS RNP APCH down to LPV or LNAV minima with a course change at the FAF or a RF-leg ending at the FAF	ICAO PANS OPS 8168
RNAV specification	See Navigation specification	ICAO PBN Manual 9613
RNP specification	See Navigation specification	ICAO PBN Manual 9613
RNP operations	Aircraft operations using an RNP system for RNP navigation applications	ICAO Doc 9613 PBN Manual
RNP route	An ATS route established for the use of aircraft adhering to a prescribed RNP navigation specification	ICAO Doc 9613 PBN Manual
RF – Radius to Fix path terminator	– An ARINC 424 specification that defines a specific fixed-radius curved path in a terminal procedure. An RF leg is defined by the arc centre fix, the arc initial fix, the arc ending fix and the turn direction.	ICAO Doc 9613
RNAV Approach	This is a generic name for any kind of approach that is designed to be flown using the on-board area navigation system. It uses waypoints to describe the path to be flown instead of headings and radials to/from ground-based navigation aids. RNP APCH navigation specification is synonym of the RNAV approach.	ICAO Doc 9613
RNP APCH – RNP approach	The RNP navigation specification that applies to approach applications based on GNSS. As illustrated in figure 2 below, there are four types of RNP APCH that are flown to different minima lines published on the same RNAV(GNSS) approach chart.	ICAO Doc 9613

SBAS – Satellite-Based Augmentation System	A wide coverage augmentation system in which the user receives augmentation information from a satellite-based transmitter. (ICAO Annex 10). The European SBAS is called EGNOS, the US version is called WAAS and there are also other SBASs in different regions of the World such as GAGAN in India and MSAS in Japan	ICAO Doc 9613

Table 28: Glossary of terms

Acronym	Definition
AGL	Above Ground Level
APCH	Approach
APP	Approach
APV	Approach Procedure with Vertical Guidance
ATM	Air Traffic Management
CNS	Communication Navigation and Surveillance
CONOPS	Concept of Operations
CR	Change Request
DPIFR	Dual Pilot IFR
EATMA	European ATM Architecture
E-ATMS	European Air Traffic Management System
FATO	Final Approach and Takeoff
FL	Flight Level
FND	Flight and Navigation Display
GBAS	Ground Based Augmentation System
GND	Ground
HDD	Head Down Display
HUD	Head Up Display
HPAR	Human Performance Assessment Report
ICAO	International Civil Aviation Organization
IDF	Initial Departure Fix
IFR	Instrument Flight Rules
IMC	Instrument Meteorological Conditions
ILS	Instrument Landing System

INTEROP	Interoperability Requirements
KPA	Key Performance Area
MCA	Minimum Crossing Altitude
OFA	Operational Focus Area
OI	Operational Improvement
OPAR	Operational Performance Assessment Report
OSED	Operational Service and Environment Definition
PAR	Performance Assessment Report
PIRM	Programme Information Reference Model
QoS	Quality of Service
RF	Radius to Fix
RNP	Required Navigation Performance
SAC	Safety Criteria
SAR	Safety Assessment Report
SecAR	Security Assessment Report
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SPIFR	Single Pilot IFR
SPR	Safety and Performance Requirements
SWIM	System Wide Information Model
TLOF	Touchdown and Liftoff Area
TS	Technical Specification
VAPP	Vertical Approach
VFR	Visual Flight Rules
VMC	Visual Meteorological Conditions

Table 29: List of acronyms

6 References

6.1 Applicable Documents

Safety Methodology and Assessment Practices

[1] Safety – Guidance Reference Material, Edition 4.0

[2] Safety - Guidance to Apply the Safety Reference Material, Edition 3.0

[3] Safety – Guidance to Resilience Engineering

[4] Accident Incident Model for En-Route, Edition 2017

[5] Accident Incident Model for Controlled Flight into Terrain, Edition 2017

Performance

[6] PJ.19 Validation Targets (2019), Edition 00.01.00

6.2 Reference Documents

[7] Eurocontrol Skybrary, https://www.skybrary.aero/index.php/Main_Page#operational-issues

[1] SESAR Solution PJ.01-06 SPR-INTEROP/OSED for V3 - Part I (D5.1.010)

[2] SESAR Solution PJ.01-06 SPR-INTEROP/OSED for V3 - Part II (D5.1.010)

[3] SESAR Solution PJ.01-06 SPR-INTEROP/OSED for V3 - Part IV (D5.1.010)

[4] SESAR Solution PJ.01-06 Validation Plan (VALP) for V3 – Part I (D5.1.020)

[5] SESAR Solution PJ.01-06 Validation Plan (VALP) for V3 – Part II (D5.1.020)

[6] SESAR Solution PJ.01-06 Validation Plan (VALP) for V3 – Part IV (D5.1.020)

[7] SESAR Solution PJ.01-06 Validation Report (VALR) for V3 – (D5.1.050)

[8] SESAR Solution PJ.01-06 CBA for V3 (D5.1.040)

Appendix A Safety Objectives

A.1 Safety Objectives (Functionality and Performance)

ID	Description
SO-0001	FCRW monitoring during advanced PinS operation shall be effective
SO-0002	Trajectory management by FCRW shall be effective during advanced PinS operation
SO-0003	Trajectory management by A/C systems shall be effective during advanced PinS operation
SO-0004	FCRW shall revert to contingency procedures in case of loss of GNSS during advanced PinS operation
SO-0005	FCRW shall be supported by HMD in case of DVE
SO-0006	FCRW shall revert to contingency procedures in case of loss of HMD during advanced PinS operation.
SO-0007	FCRW shall revert to contingency procedures in case of loss of AP during advanced PinS operation

A.2 Safety Objectives (Integrity)

ID	Description
SO-0101	Frequency of occurrence of helicopter deviating laterally or vertically from A-PinS towards terrain in controlled airspace leading to CFTT shall not be greater than 2x10-7/flight.

Appendix B Consolidated List of Safety Requirements

B.1 Safety Requirements (Functionality and Performance)

ID	Description
SR-1001	FCRW shall be able to detect lateral route deviation greater than 0.3Nm including during RF leg using HDD or HMD
SR-1002	FCRW shall be able to detect lateral and vertical route deviation during final LPV approach using HDD or HMD
SR-1003	The HMD symbology shall help the pilot to control laterally and vertically the trajectory and shall indicate the flight parameters (speed, altitude, velocity vector…) at any time
SR-1004	RNP system shall be approved in accordance with the RNP 0.3 navigation specification
SR-1005	FMS system shall be approved for RNP approach down to LPV minima
SR-1006	RNP system coupled with AP /FD shall be capable of executing RF legs
SR-1007	The FMS shall provide advanced PinS guidance during the curved segment between the Intermediate Fix and the Final Approach Fix, which combines longitudinal, lateral and vertical movements.
SR-1008	Helicopter operator shall define contingency procedure in case of loss of GNSS and/or SBAS during A-PinS operations and considering local environment
SR-1009	In case of loss of GNSS and/or SBAS during PinS operation, FCRW shall respect helicopter operator’s contingency procedures (e,g, conventional navigation or dead reckoning)
SR-1010	The status of GNSS/SBAS (vertical guidance) shall be displayed to the FCRW at any time
SR-1011	The HMD shall visually provide all relevant data when approaching the missed approach point to support the FCRW in the decision whether to continue or abort the approach procedure
SR-1012	Helicopter operator shall define contingency procedure in case of loss of HMD during A-PinS operations and considering local environment
SR-1013	In case of loss of HMD during PinS operation, FCRW shall respect helicopter operator’s contingency procedures
SR-1014	The status of HMD shall be displayed to the rotorcraft pilot at any time.

SR-1015	Helicopter operator shall define contingency procedure in case of loss of AP during A-PinS operations and considering local environment
SR-1016	In case of loss of AP during PinS operation, FCRW shall respect helicopter operator's contingency procedures

B.2 Safety Requirements (Integrity)

ID	Description
SR-1101	HMD data corruption shall occur less than 1*10-7.

Appendix C Assumptions, Safety Issues & Limitations

C.1 Assumptions log

The following Assumptions were necessarily raised in deriving the above Functional and Performance Safety Requirements:

Ref	Assumption	Validation
N/A	N/A	N/A

Table 30: Assumptions log

C.2 Safety Issues log

The following Safety Issues were necessarily raised during the safety assessment:

Ref	Safety issue	Resolution
N/A	N/A	N/A

Table 31: Safety Issues log

C.3 Operational Limitations log

The following Operational Limitations were necessarily raised during the safety assessment:

Ref	Operational Limitations	Resolution
N/A	N/A	N/A

Table 32: Operational Limitations log

-END OF DOCUMENT-